(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 164 576 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.12.2001 Bulletin 2001/51

(21) Application number: **00128291.2**

(22) Date of filing: **22.12.2000**

(51) Int Cl.[7]: **G10L 17/00**, H04M 3/38, H04M 3/493, G07C 9/00, G06F 1/00

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **15.06.2000 EP 00112666**

(71) Applicant: **Swisscom AG**
3050 Bern (CH)

(72) Inventor: **Van Kommer, Robert**
1752 Villars-sur Glâne (CH)

(74) Representative:
Saam, Christophe, Patents & Technology Surveys Ltd.
Faubourg du Lac 2
2001 Neuchâtel (CH)

(54) Speaker authentication method and system from speech models

(57) Speaker authentication method in a voice portal (3), comprising the following successive steps:

(1) storing at least an utterance of one user of said portal in said portal (22),
(2) subsequently requesting said user to utter choices in a voice menu (26),
(3) subsequently adapting said user's speech models with said choices uttered by said user (50),
(4) using said adapted speech models for authenticating said user using said utterance stored in said portal (48).

EP 1 164 576 A1

Descripti n

[0001] Th pres nt invention concerns a speaker authentication m th d and syst m. More specifically, the present inv ntion concerns a multi-pass speech recognition and sp ak r authentication method for us r auth ntication in a voice portal, and an improved voice portal.

Prior art

[0002] Voice portals, for example in interactive voice response systems, are already known in which information can be stored and accessed by a plurality of users with spoken requests directly uttered in a microphone or transmitted through the telephone network and interpreted in the voice portal. Voice portals have the advantage that the information can be accessed without any prior knowledge and without any special equipment from any telephone terminal in the world.

[0003] Voice portals often can give access to confidential information, for example bank or medical information. The level of confidentiality, and the kind of information which may be stored in a voice portal, thus critically depend on a reliable identification of the authorized users, in order to authorize them or not.

[0004] In many conventional systems, users have to enter or to confirm their identity with a user identification and/or a password entered as DTMF codes on the keypad of the users' equipment. In many situations, like e.g. in cars, this solution proves unpractical. Moreover, user identifications and passwords are hard to remember and are often written down near the user's equipment, resulting in weak security.

[0005] It has already been suggested to authenticate users with a spoken identity uttered at the entry point of the dialogue with the voice portal. Speech recognition techniques have been used for recognizing the claimed identity and speaker verification techniques for verifying the claimed identity. In the next dialogue turn, the user is accepted or rejected if he is not registered in the portal or if the claimed identity cannot be verified.

[0006] Currently, the major trend in speech recognition and speaker verification technology is the Hidden Markov Model. This statistical method describes speech by a sequence of states (Markov states). These are linked by transition probabilities, to move from state to state and each state emits, via a certain probability distribution, a speech vector. Among the many weaknesses of HMMs, one could mention the poor robustness against a typical mismatch situation (the training and testing speech material is different). In the last years of research in the field of speech recognition, many researchers have concluded that the robustness of current methods is far from being comparable to what human beings could achieve.

[0007] Different methods have already been described to improve the robustness of speech recognition. It is known that the speaker verification accuracy improves when more speech material is available. Furthermore, some systems achieve better performance by using speaker-dependent speech models, which are usually learned during an enrollment session. However, most users would not accept having to spend the time necessary for this session. Besides, speaker-dependent recognition can only be used once the speaker has been identified, but not for recognizing the identity claimed by the user during the first turn of a dialogue.

[0008] Instead of learning a complete set of speech models for each user, several adaptation techniques have been described for adapting a good speaker-independent model set to a new speaker. If the adaptation data is available in one block, e.g. from a speaker enrollment session, one may use static adaptation methods. Alternatively, adaptation can proceed incrementally as adaptation data becomes available (incremental adaptation). In the case where the true transcription of the adaptation data is known, then it is termed supervised adaptation, whereas if the models are adapted with unlabelled speech material, then it is termed unsupervised adaptation. Known adaptation techniques comprise maximum likelihood linear regression (MLLR) techniques and maximum a posteriori (MAP) adaptation.

[0009] Other adaptation techniques do exist to adapt the models with the current noise captured from the line. Many systems are using a short moment of silence to do the modeling. That particular model is then combined with the original one. A two-pass system is described in the patent application EP-A2-0880126 which adapts the silence models by first segmenting the speech utterances and then adapting the silence modeling via unsupervised adaptation.

[0010] In a voice portal, all those adaptation techniques may be used for improving the speech models during the enrollment session and/or during the whole dialogue; the adapted models may even be stored in the system and used for speech recognition in future sessions. However, they cannot be used in each session until the speaker's identity has been recognized and/or verified.

[0011] This first dialogue turn is thus very critical since only speaker-independent recognition techniques can be used and since the perplexity (number of possible branching) of the identity input is, at least, proportional to the number of users. Conversely, in the rest of the spoken dialogue, the speech recognition has an easier task; the perplexity is lower.

Summary of the invention

[0012] One aim of the invention is to provide a voice portal system and method with improved speaker authentication performances over existing methods and systems.

[0013] One other aim is to provide a speaker-dependant verification method in a voice portal system which allows for an accurate speaker recognition and verification based on an utterance spoken by the user during the first dialogue turn.

[0014] In accordance with one embodiment of the present invention, a speaker authentication method is provided in which a special dialogue has been designed in order to collect more data and to adapt the speech and silence models used for the first dialogue turn.

[0015] According to another aspect of the invention, a multi-pass speech recognition scheme is used to improve the adaptation of speech models.

[0016] According to another aspect of the invention, a speaker authentication method in a voice portal is provided, which comprises the following successive steps:

(1) storing at least an utterance of one user of said portal in said portal,
(2) subsequently requesting said user to utter choices in a voice menu,
(3) subsequently adapting said user's speech models with said choices uttered by said user,
(4) using said adapted speech models for authenticating said user using said utterance stored in said portal.

[0017] According to another aspect of the invention, a spoken dialogue is constructed that enables a delayed answer upon the user's speech input. As a matter of fact, in most applications of voice portals, a reliable user authentication is only needed for the delivery of security-critical information or for specific transactions that are usually carried out only after a few selections in the voice menu. Therefore, the user authentication can be postponed till that later point in the dialogue.

[0018] Moreover, user authentication may be purely suppressed if the critical dialogue portion is not reached.

[0019] According to another aspect of the invention, the speech models used for speaker authentication are adapted during the spoken dialogue. This allows to perform the speaker authentication task with new speaker-dependant and session-dependant speech models, and thus to improve the authentication accuracy.

[0020] According to another aspect of the invention, the first utterance is stored in the system in order to postpone its recognition and the verification of the user's identity until enough speech material has been collected to perform a speaker-dependant speech recognition and speaker verification. The first utterance can be normalized, multi-pass adaptation techniques can be used on it and the speech models can be adapted in order to improve the speaker authentication and speech recognition quality.

Brief description of the drawing

[0021] The invention will be described with reference to the following drawing wherein:

Fig. 1 shows a schematized representation of a possible embodiment of a voice portal according to the invention.

Fig. 2 shows a flowchart illustrating a dialogue with the inventive voice portal.

Detailed Description

[0022] Fig. 1 shows a diagram of a telecommunication system including a voice portal hosting system 3. A plurality of users can establish a voice connection with this voice portal 3 over a public telecommunication network 2, such as a public switched telecommunication network (PSTN), an integrated services data network (ISDN), a mobile telecommunication network, e.g. a GSM network, or a voice-enabled IP-Network (VoIP). The connection is established by selecting the voice portal 3 phone number on a user terminal equipment 1 such as a phone terminal. Preferably, the voice portal phone number is a free business number in the 0800 range or, in a various embodiment, a charging number in the 0900 range. The voice portal 3 may give access to information and services from one or several service providers 13 connected permanently or occasionally to the portal over the second telecommunication network 12.

[0023] The voice portal hosting system includes a dialogue manager 11 for establishing a spoken dialogue with the user 1. The dialogue manager 11 answers to commands or requests uttered by the user with the requested information or service or by establishing a new connection with an external server.

[0024] User voice requests are recognized by a speech recognizer 10 that preferably uses HMM (Hidden Markov Models), adaptive neural networks or hybrids networks. In a preferred embodiment, the speech recognition modul

comprises Hidden Markov Models built with a toolkit such as th HTK toolkit.

[0025] A s lector 9 can select speaker-indep ndent speech mod ls 7 or, as so n as the us r has been id ntified, us r-depend nt speech mod ls 8. User-dep ndent speech models usually allow for a fast r and mor reliable speech recognition than user-indep ndent speech mod ls, but can bviously only b us d aft r us r identification.

[0026] At least th first utterance sp k n by the us r during a sessi n, but preferably all th us r utterances, ar stored in a temporary memory 5 and us d by a speech mod ls adaptation module 60 for improving th quality of th speech recognition and speaker authentication performed by the modules 10 and 6 respectively. As will b explain d later, at least some utterances are stored in order to be recognized or to serve for an authentication using improvements of the speech models gained from subsequent utterances.

[0027] The user is identified and preferably authenticated by a speaker authentication module 6. The speaker authentication module preferably uses HMM (Hidden Markov Models), but could possibly use adaptive neural networks or hybrids networks. In a preferred embodiment, the speaker authentication module 6 comprises Hidden Markov Models built with a toolkit such as the HTK toolkit. In a preferred embodiment, the user identity is first recognized from the text corresponding to the utterances spoken using speaker-independent speech models, for example using the speech models 7. An active verification signal Verif is delivered as soon as the identity of the calling user is known. Speaker-dependant speech models 8 can be selected by the selector 9 and used by the speech recognizer 10 as soon as the signal Verif is active. The user identity is then verified in order to authenticate the user with an improved reliability; an authentication signal Auth becomes active when the user has been authenticated with the required confidence level.

[0028] Instead of collecting speaker-dependant speech models in the speaker-dependent database 8 during an enrolment session, adaptation techniques can be applied for improving the models available for speech recognition and speaker authentication. In this case, by using only a small amount of data from a new user, the speaker-independent model 7 can be adapted using maximum likelihood linear regression (MLLR) to fit the characteristics of each user. This adaptation can proceed incrementally as adaptation data becomes available (incremental adaptation).

[0029] The speech models used on each utterance for recognition and/or authentication are adapted during each session with the voice material stored in the temporary memory 5, as will be explained later. A second pass may be used on the first utterances for improving the recognition and/or authentication reliability using subsequently spoken voice material. The segmentation of the utterances may be improved with subsequent voice choices. A normalization of the speech segments may also be performed. New speech models, including for example new silence models, which are better adapted to the channel currently used, may be created from subsequent utterances and added to the set of models used for recognizing the first utterances and for authenticating the user from those utterances.

[0030] The speaker authentication module 6 and the speech recognizer 10 can be combined into one single module. The speaker authentication module may use additional information, for example data transmitted over a signalization channel such as the caller terminal identification, for example the CLI in a fixed network, the IP address in an Internet network or the IMSI (International Mobile Subscriber Identification) in a mobile network, in order to make easier the user identification/authentication task.

[0031] The confidence level needed for authenticating the user can preferably be set by the dialogue manager and/or by the operator of the voice portal 3, for example a service provider 13, depending on the requested security. A USER signal unambiguously indicates the user identified and/or authenticated by the module 6.

[0032] Several methods can be used independently or simultaneously for improving the authentication and recognition of the first utterance based on subsequent utterances:

1. Subsequent normalization techniques

[0033] Several normalization techniques (CMN, Energy normalization) can be applied within the inventive dialogue design. These normalization techniques work only when enough speech material is available to estimate the needed values of energy means or cepstral coefficients. In conventional voice response systems, these techniques are not used because they induce unacceptable delays in the dialogue interaction.

[0034] According to the invention, the user's first utterance is normalized using subsequent speech material, for example choices in a voice menu, uttered by the user. This allows for a more accurate speech recognition and speaker identification/verification algorithm.

2. Multi-pass adaptation techniques

[0035] Figure 2 illustrates a specifically adapted dialogue between the user 1 and the inventive voice portal 3. The dialogue has been adapted in the sense that the dialogue manager will activate the final pass of the speech recognition and authentication process only when the user reaches a critical part of the dialogue.

[0036] The one skilled in the art will understand that, besides th improved us r-int rface, wh n this dial gu design is applied, many fficient speech recognition techniques can be appli d to improv th perceived quality f the voice

interaction.

1. During the first step 20, at the entry point of a personal voice portal, the user selects the voice portal 3 phone number in the network 2 and the call is established. The user is then requested to utter his user identification and/or password. The speech material and channel is is collected and stored in the temporary memory 5 during step 22. No decision about the rejection of the user is made at this point of the dialogue. The claimed identity will only be verified later on, with known speaker verification methods, when the following conditions have been met:

- The user wants to access a secure portion of the voice menu, and
- The user's speech models have been adapted with subsequent speech material, and/or
- Enough speech material has been collected from said user to allow for reliable speaker verification.

2. Two processes are then performed in parallel in the voice portal 3. In the first process, the user is given access to a free portion of the voice menu (step 24). This free portion may include for example access to non-confidential information from the service provider 13. The user can utter choices in this menu (step 26); speech material is collected in the memory 5. The dialogue proceeds with subsequent questions and answers by using speaker-independent speech recognition (step 30) as long as the user has not been identified.

In a preferred embodiment, the user is provisionally recognized during steps 26-30 using for example a speaker-independent recognition of the text corresponding to the first utterance or non-speech elements such as the CLI, IMSI or IP terminal identification. The provisory identity is used in order to retrieve from the user profile database the user's speech and/or language models 8 used for improving the speech recognition accuracy during the dialogue, and will be verified later on, when needed, using known speaker verification methods in order to authenticate the user. Test 28 denotes a check of the Verif signal, which indicates if the user has already been identified and if speaker-dependant recognition algorithms can be used during step 32 for speech recognition.

In another embodiment, an incremental adaptation technique is used for improving the speech model used for each turn of the dialogue. Supervised adaptation techniques are preferably used if the user's answers can be expected (for example for choices in a closed menu list).

3. In a concurrent task within the system, the authentication flag Auth is initially reset (step 42). During step 44, the authentication module then tries to identify (step 440) and to authenticate (step 442) the user 1 using the first utterance spoken during the first exchange. Apart from the user's voice, other elements such as the terminal identification (CLI, IMSI, IP-address, etc.) may be used in order to help in the identification and authentication process.

At least the first utterance, but preferably all speech inputs, is first segmented via a speaker-independent speech recognizer. The speech segments and non-speech signals are then used to adapt the speech/silence models via an adaptation technique like for instance MLLR.

4. For speech models, only the segments with an acceptable confidence level are used to provide supervised adaptation of model parameters. Unsupervised techniques may also be applied.

5. Subsequent recognition/adaptation passes may be performed during step 50 to further improve (i) the confidence level of the recognition and authentication system, (ii) the segmentation, and (iii) the adaptation of speech and silence models. In the case where the user number is composed of a digit string, the subsequent recognition passes are stopped when the error detection code grants permission.

6. As the dialogue reaches the critical security point (step 34) in the menu where a user authentication is requested in order for example to access more confidential information or to perform financial transactions, the final recognition and verification pass is processed and the user may be rejected from the service at this point.

If the user has already been authenticated at this stage, he is given access to the secure portion of the voice menu (step 40). Otherwise, access is denied, or the user may be given a second try or requested to authenticate himself using another method, for example by uttering a password or entering a DTMF-PIN code on the keypad of his equipment (step 38).

In the preferred embodiment illustrated in Figure 2, a succession of authentication passes 44 are iteratively performed while the user is navigating through the voice menu, until a predefined confidence level has been reached (test 46). The authentication flag is set when this level has been reached (step 48); otherwise an additional adaptation pass is performed (step 50). No access to secure portions of this menu is allowed until the user has been reliably authenticated. It is also possible to build a voice menu with a plurality of portions with different security

r quirem nts, different confid nce lev ls for the user authenticati n being required for accessing said different portions.

Thus, according to the invention, a v ry reliabl user v rification and a v ry accurat recognition f th first utterance can be performed, based on more sp ech material and using speech models adapted t th current sp aker.

7. In the dialogue, there is no turn to explicitly accept the user. He is accepted by default.

The method uses the well-known fact that the accuracy of speaker-dependent speech recognition is higher than that of speaker-independent systems.

In the case of personal voice portals, the present invention uses several spoken utterances (as many as possible) to adapt the speech models to the speaker, and therefore postpones the decision till the user wants to access the secure portion of the voice menu. In a sense, it acts precisely as a fast on-line enrollment session.

The techniques 1 (subsequent normalization) and 2 (multi-pass adaptation) may be combined to achieve increased performance.

3. Improved speaker verification

[0037] During the elapsed time between the first dialogue turn and the critical security point, several command words may be used to complement the rejection/acceptation decision of the server system. In order to implement this additional verification scheme, the spoken command words of each session have to be stored within the authentication system and the authentication system extracts from them the model needed for the speaker verification procedure. In fact, these command words are used to create additional speech material for speaker verification. It is well known that, just as the speaker adaptation improves with the availability of more data, speaker verification improves equally with the increasing quantity of speech material.

[0038] The combination of all three methods contributes to improve the overall perceived quality of service.

[0039] As mentioned above and from the dialogue perspective, another obvious advantage is to improve the dialogue, since the rejection/acceptation dialogue is simply skipped in most cases. The dialogue is shorter and therefore more efficient.

[0040] In some cases and for some particular model parts, a higher adaptation speed has been measured with simpler models. The technique is used, for instance, for silence models adaptation.

Example of implementation

[0041] At least some of the voice applications performed by the dialogue manager include voice-enabled e-commerce applications. The following example of implementation is about a banking teleservice. The user wishes to know the amount of money left on his bank account.

The user	The banking teleservice
The user calls the banking service via the voice portal and from his hotel room.	
	The system: *Welcome to the banking service, please state your user number.*
The user: *3 4 6 1 2 4 9 3*	
	The system: *What kind of service do you want: Information on new services, information about your account, or would you like to transfer money?*
The user: *I would like information about my account*	
	The system: *Would you like to know the current account status or the latest transactions that have occurred.*
The user: *I would like to know the current account status*	

(continued)

The user	The banking teleservice
	The verification of the claimed identity is now performed. The three sentences are used to adapt the speech and silence models. Additionally, the authentication system uses the digit string of the user number as well as the two subsequent sentences to infer if the user's claimed identity is correct.
	The system: *On the account number 3 4 6 1 2 4 9 3, the available amount is 4345.80 CHF.*
The user terminates the communication.	

[0042] The voice portal 3 may comprise a standard digital computer including an internal memory (not shown) in which a computer program product can be directly loaded for performing the method steps of the invention when said program is run on said computer.

Claims

1. Speaker authentication method in a voice portal (3), comprising the following successive steps:

   (1) storing at least an utterance of one user of said portal in said portal (22),
   (2) subsequently requesting said user to utter choices in a voice menu (26),
   (3) subsequently adapting said user's speech models with said choices uttered by said user (50),
   (4) using said adapted speech models for authenticating said user using said utterance stored in said portal (442).

2. Method according to claim 1, further repeating said steps 2 to 4 until a predefined confidence level has been reached for the authentication of said user.

3. Method according to one of the preceding claims, in which the identity of said user is first recognized and then verified using said adapted speech models for authenticating said user.

4. Method according to one of the preceding claims, in which the identity of said user is recognized from the text corresponding to said utterance.

5. Method according to the preceding claim, in which the identity of said user is recognized from the text corresponding to said utterance using speaker-independent voice recognition algorithms.

6. Method according to the claim 4, in which the identity of said user is recognized from the text corresponding to said utterance using said adapted speech models.

7. Method according to one of the preceding claims, in which the identity of said user is recognized using text-independent speaker verification.

8. Method according to claim 3, in which the identity of said user is determined using data transmitted over the signaling channel.

9. Method according to the preceding claim, wherein said data include the CLI terminal's identification.

10. Method according to one of the preceding claims, wherein user-dependant speech models (8) are stored in said portal and retrieved as soon as said user has been identified in order to improve subsequent speech recognition and/or the verification of the user's identity.

11. Method according to the preceding claim, in which said user-dependant speech models are adapted using said

choices utt red by said us r.

12. M thod according to on of the preceding claims, wh r in th identity of said user is v rifi d using said adapted speech models.

13. Method according to the prec ding claim, wh rein said user is auth nticated using supervised speech models adaptation algorithms.

14. Method according to one of the preceding claims, wherein said user is authenticated and/or verified using Hidden Markov Models and wherein said speech models are adapted using an adaptation technique of Hidden Markov Models.

15. Method according to the preceding claim, wherein said speech models are adapted using MLLR adaptation techniques.

16. Method according to the preceding claim, wherein said choices are used for adapting the speech models and therefore improving the segmentation of said utterance stored in said portal.

17. Method according to one of the preceding claims, wherein said user's utterance is normalized with subsequent speech material from said user.

18. Method according to one of the preceding claims, wherein new speech models are created from said subsequently uttered user choices.

19. Method according to the preceding claim, wherein said new speech models include silence models.

20. Method according to one of the preceding claims, wherein said user is prompted to utter his identity immediately after a connection has been established with said voice portal, said identity being stored as said utterance.

21. Method according to one of the preceding claims, wherein said user is only authenticated when he wants to access a secured portion of said voice menu.

22. Method according to one of the preceding claims, in which a plurality of portions with different security requirements have been defined in said voice menu,
and in which different confidence levels for said user authentication are defined for accessing said different portions of said voice menu.

23. Speech recognition method in a voice portal, comprising the following successive steps:

(1) storing at least an utterance of one user of said system in said portal,
(2) subsequently requesting said user to utter choices in a voice menu,
(3) subsequently adapting the user's speech models with said choices uttered by said user,
(4) subsequently using said adapted speech models for recognizing said utterance stored in said portal.

24. Computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the steps of one of the preceding claims when said product is run on an interactive voice response system connected to a first telecommunication network.

25. Voice portal (3), comprising:

a speaker authentication module (6) comprising Hidden Markov Models for authenticating users of said portal,
a dialogue manager (11) for managing a dialogue between said system and users (1) of said system, wherein said dialogue enables access to at least one secured portion in said system,
an adaptation module (60) for adapting said Hidden Markov Models,

wherein said dialogue manager enables a dialogue in which said user authentication only happens when said us r requests access to said secured portion, based on at l ast on first utt rance uttered at th beginning of said dialogue and stored in said portal.

26. Voice portal according to claim 25, wherein said authentication is performed with said at least one first utterance and using adaptation of speech models based on subsequent speech material from said user.

27. Voice portal according to claim 25, wherein said at least one first utterance is normalized with subsequent speech material from said user.

28. Voice portal according to claim 25, wherein said speech material is used for adapting the speech models and therefore improving the segmentation of said utterance stored in said portal.

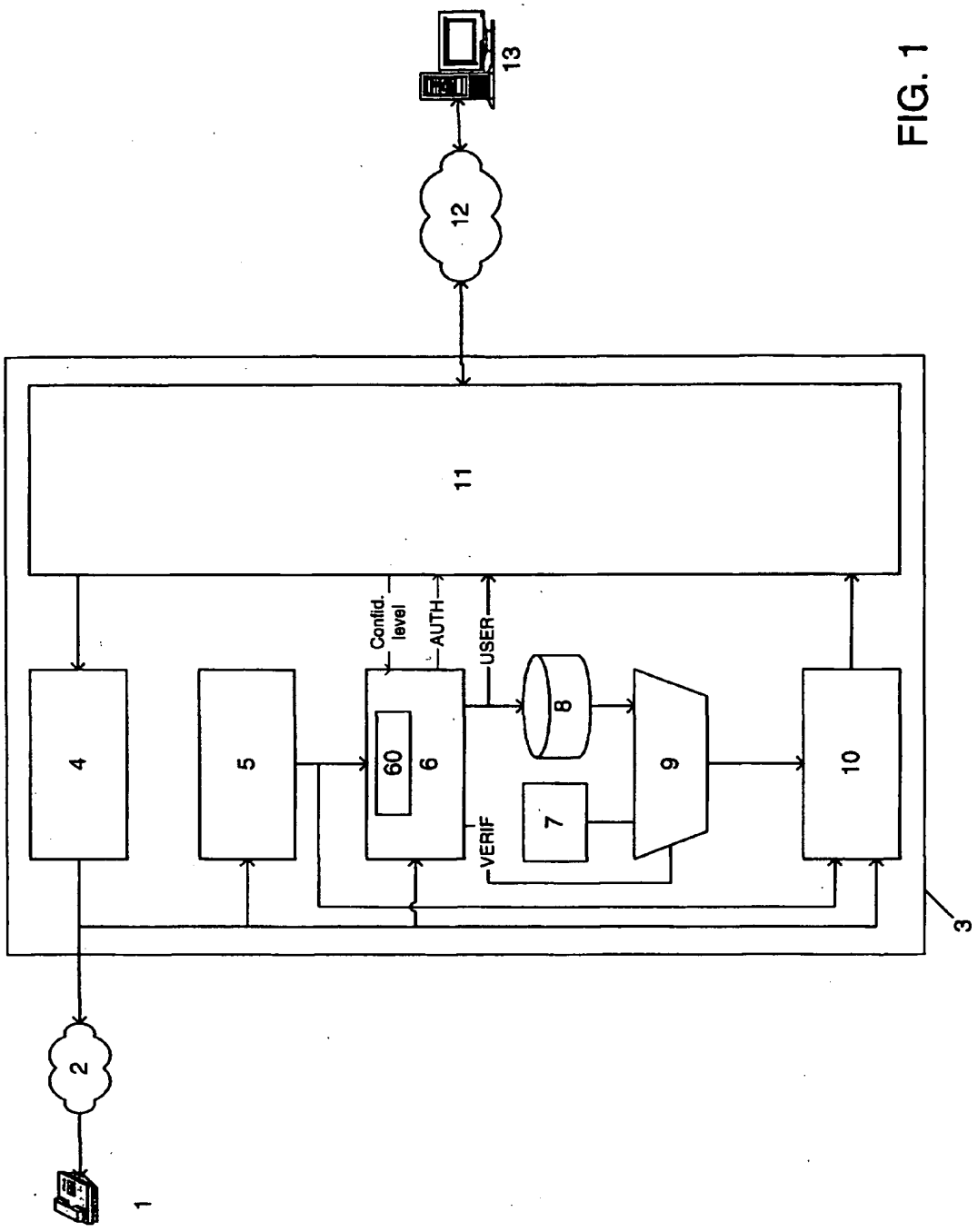

FIG. 1

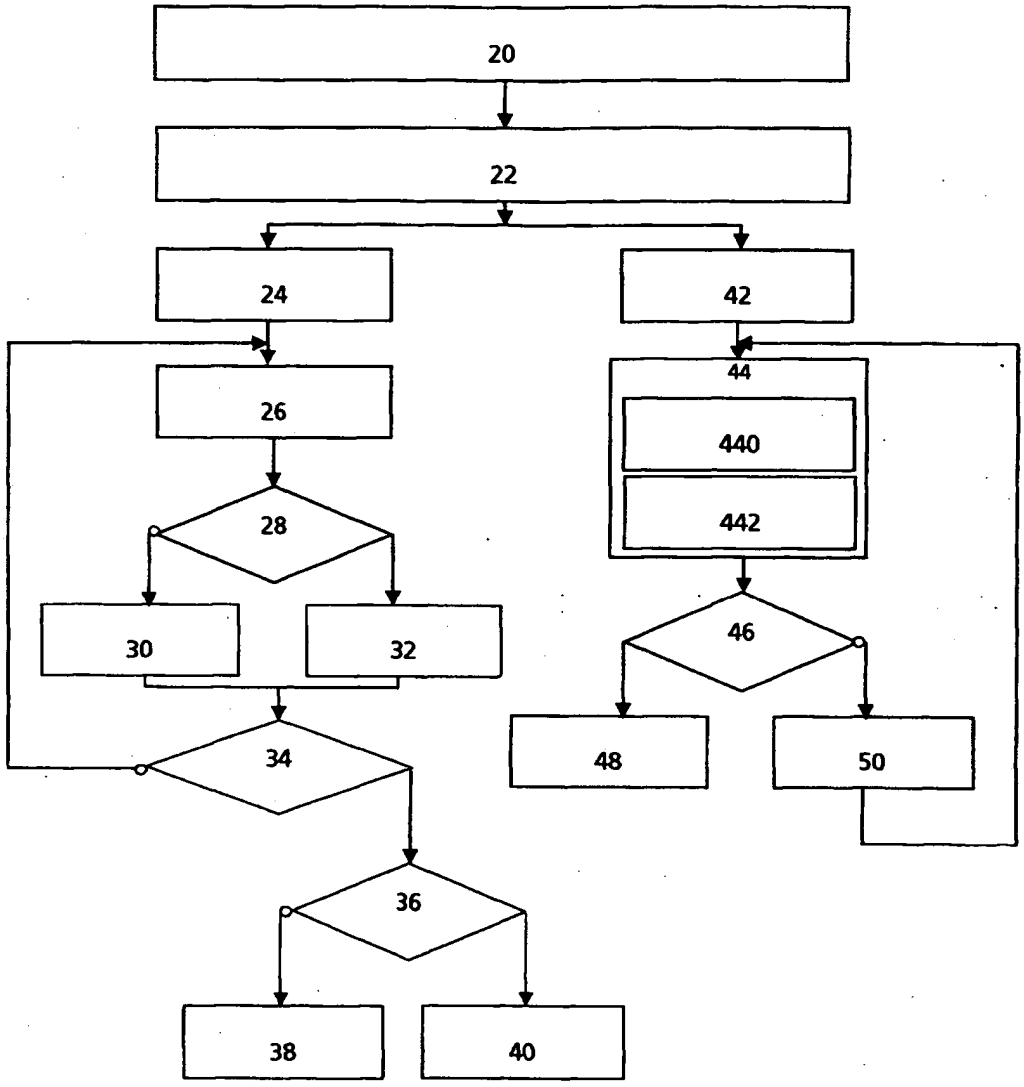

FIG. 2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 12 8291

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	WO 99 00719 A (LERNOUT & HAUSPIE SPEECHPROD) 7 January 1999 (1999-01-07) * abstract; figures 2-4 *	1-28	G10L17/00 H04M3/38 H04M3/493 G07C9/00
A	US 6 081 782 A (RABIN MICHAEL D) 27 June 2000 (2000-06-27) * abstract; figures 3,5 * & EP 0 686 297 A 13 December 1995 (1995-12-13)	1-28	G06F1/00
A	FURUI S: "Recent advances in speaker recognition" PATTERN RECOGNITION LETTERS, NORTH-HOLLAND PUBL. AMSTERDAM, NL, vol. 18, no. 9, 1 September 1997 (1997-09-01), pages 859-872, XP004102227 ISSN: 0167-8655 * page 861, right-hand column, paragraph 1.5.2 * * page 865, right-hand column, paragraph 2.4 * * page 867, right-hand column, paragraph 2.5 *	14,17,25	
A	SUNGJOO AHN ET AL: "Effective speaker adaptations for speaker verification" 2000 IEEE INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH, AND SIGNAL PROCESSING. PROCEEDINGS (CAT. NO.00CH37100), ISTANBUL, TURKEY, 5-9 JUNE 2000, pages II1081-II1084 vol.2, XP002180588 2000, Piscataway, NJ, USA, IEEE, USA ISBN: 0-7803-6293-4 * abstract *	15	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
G10L
H04M
G07C
G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	19 October 2001	Quélavoine, R

CATEGORY OF CITED DOCUMENTS
X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 12 8291

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-10-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9900719 A	07-01-1999	AU 8125198 A	19-01-1999
		EP 0991990 A1	12-04-2000
		WO 9900719 A1	07-01-1999
US 6081782 A	27-06-2000	AU 673480 B2	07-11-1996
		AU 1445395 A	17-07-1995
		CA 2156610 A1	06-07-1995
		CN 1118633 A	13-03-1996
		DE 69425818 D1	12-10-2000
		DE 69425818 T2	18-01-2001
		DK 686297 T3	16-10-2000
		EP 0686297 A1	13-12-1995
		ES 2150549 T3	01-12-2000
		JP 8507392 T	06-08-1996
		NZ 278267 A	27-07-1997
		WO 9518441 A1	06-07-1995

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82